REMARKS

This paper is submitted in response to the New Grounds of Rejection set forth in the Decision on Appeal dated January 12, 2010 ("Decision"), and is being submitted with a Request for Continued Examination (RCE) within two months of the Decision for the above-captioned U.S. patent application. In this response, Applicants have amended Claims 1, 15 and 21 to clarify that which Applicants consider to be the presently-claimed invention. Applicants respectfully submit that the amendments to the claims are fully supported by the originally-filed specification.

As set forth in the Decision, the Board of Patent Appeals and Interferences reversed the Examiner's rejections of Claims 1-4, 6-27 and 29-34 but raised New Grounds of Rejection. Applicants are submitting this paper with appropriate amendments and remarks made herein to address the New Grounds of Rejection of Claims 1 and 15-21, as set forth on pages 12-15 of the Decision, and to reopen prosecution and have the matter reconsidered by the Examiner.

The rejection of Claims 1, 15, and 21 under 35 U.S.C. § 103(a) as being unpatentable over admitted prior art ("APA", the originally filed application at page 1, lines 19-33), U.S. Patent No. 4,919,545 (hereinafter "Yu"), and U.S. Patent No. 6,061,753, (hereinafter "Ericson") is hereby traversed and reconsideration thereof is respectfully requested.

Claim 1, as amended herein, recites a data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network, the method comprising steps of: providing, by the storage system to one of the at least two devices, a set of identifiers having a number of identifiers equal to a maximum number of permissible outstanding requests for the one of the at least two devices; receiving over the network at the storage system a request from the one of the at least two devices for access to at least one of the plurality of volumes of the storage system, the request identifying the at least one of the plurality of volumes in the storage system and a represented source of the request and including an encrypted one

of the identifiers of the set, each identifier in the set used to authenticate a different request from the one of the at least two devices; and selectively servicing the request, at the storage system, based at least in part on steps of: determining, from configuration data, whether the represented source is authorized to access the at least one of the plurality of volumes; and verifying that the represented source of the request is the one of the at least two devices that issued the request, said verifying including determining whether the encrypted one of the identifiers is a next expected identifier of the set.

Claim 15, as amended herein, recites a computer readable medium comprising stored thereon: a first data structure to manage accesses by a plurality of devices to volumes of data at a storage system over a communication network, the first data structure comprising a plurality of records corresponding to the plurality of devices, the plurality of records comprising at least one record corresponding to a first of the plurality of devices and including configuration information having at least one identifier that identifies which of the volumes of the storage system the first of the plurality of devices is authorized to access, and authentication information; code that provides to the first of the plurality of devices a set of identifiers having a number of identifiers equal to a maximum number of permissible outstanding requests for the first of the plurality of devices; code that manages access to the plurality of volumes of the storage system responsive to requests, each of said requests identifying one of the plurality of volumes to be accessed and one of the plurality of devices that is represented as having issued said each request, each of said requests from the first of the plurality of devices also including an encrypted one of the identifiers of the set, each identifier in the set used to authenticate a different request from the first of the plurality of devices; code that uses the authentication information to determine whether one of the plurality of devices identified by one of the requests as having issued said one request is the first of the plurality of devices; and code that determines, for a first of said requests from the first of the plurality of devices, whether the first request includes an encrypted one of the identifiers which is a next expected identifier of the set.

Claim 21, as amended herein, recites a storage system comprising: at least one storage device apportioned into a plurality of volumes; a configuration table to store configuration data identifying which of a plurality of devices coupled to the storage system via a network are authorized to access which of the plurality of volumes; a component that provides, to a first of the plurality of devices, a set of identifiers having a number of identifiers equal to a maximum number of permissible outstanding requests for the first device; and a filter, responsive to the configuration data, to selectively forward to the at least one storage device requests for access to the plurality of volumes received from the plurality of devices over the network, wherein each request identifies at least one of the plurality of devices that is represented to the storage system as having issued the request, and wherein the filter is adapted to verify that the at least one of the plurality of devices identified in the request is the device that issued the request, each request from said first device including an encrypted one of the identifiers of the set, each identifier in the set used to authenticate a different request from the first device, the filter adapted to determine whether each request from the first device includes an encrypted one of the identifiers which is a next expected identifier of the set.

Ericson discloses a method, apparatus, and computer program product for controlling access to a target device utilizes an initiator identifier to either permit or deny access to a selected portion of the target device. A message having the initiator identifier is directed from the initiator device to the target device to request access to the selected portion of the target device. Upon receipt by the target device, it is determined if the initiator identifier is in a permitted set of identifiers associated with the selected portion of the target device. If the initiator identifier is in the permitted set, then access to the portion of the target device is permitted and the initiator can access the target in accordance with conventionally known processes. (See Abstract).

Yu discloses a security technique for use in an intelligent network. The security technique provides a method for authorizing access by a process located in an invocation node to an object, or a network resource, located in an execution node. The method includes the steps of granting permission to the invocation node to access the object by

transmitting a capability and a signature from the execution node to the invocation node. The capability includes a unique identifier of the object and access rights to the object. The signature is formed at the execution node by encryption of the capability with an encryption key that is unique to the invocation node and is stored only in the execution node. A request for access to the object is transmitted with the capability and the signature from the invocation node to the execution node. At the execution node, the request is authenticated by encryption of the capability with the encryption key that is associated with the invocation node to form a test signature. Access to the object is authorized only when the test signature matches the signature received from the invocation node. (See Abstract).

The APA states that with the growth of networked computer systems, multiple hosts have been coupled over a network to a shared data storage system. Fibre Channel is an example of a network that can be used to form such a configuration. Fibre Channel is a network standard that allows multiple initiators to communicate with multiple targets over the network, where the initiator and target may be any device coupled to the network. Using a network, multiple hosts are able to share access to a single storage system. One problem with coupling multiple hosts to a shared storage system is the management of data access at the storage system. Because multiple hosts have access to a common storage system, each host may physically be able to access information that may be proprietary to the other host processors. Various techniques have been implemented to manage access to data at the storage system. For example, certain portions or zones of memory at the storage system may be dedicated to one or more of the hosts. Each host is 'trusted' to access only those portions of memory for which it has privileges. However, such an approach is vulnerable to the individual actions of each of the hosts. As a result, such a data management method may not be sufficient to protect data from unprivileged accesses. (See page 1 of the originally filed application in the "Description of Related Art", lines 18-32).

Pages 12-13 of the Decision under New Grounds of Rejection contend that the above-mentioned APA teaches "determining, from configuration data, whether the

represented source is authorized to access the at least one of the plurality of volumes"; that Yu also teaches the foregoing determining step (with respect to accessing an object) and that Yu also teaches "verifying that the represented source of the request is the one of the at least two devices that issued the request"; and that Ericson teaches the remaining features of Claim 1 prior to amendment herein.

Claim 1, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references do not disclose or suggest at least the features of ***a data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network, the method comprising steps of: providing, by the storage system to one of the at least two devices, a set of identifiers having a number of identifiers equal to a maximum number of permissible outstanding requests for the one of the at least two devices; receiving over the network at the storage system a request from the one of the at least two devices for access to at least one of the plurality of volumes of the storage system, the request ... including an encrypted one of the identifiers of the set, each identifier in the set used to authenticate a different request from the one of the at least two devices; and selectively servicing the request, at the storage system, based at least in part on steps of: ... verifying that the represented source of the request is the one of the at least two devices that issued the request, said verifying including determining whether the encrypted one of the identifiers is a next expected identifier of the set,*** as recited in Claim 1.

As pointed out above, amended Claim 1 recites providing a set of identifiers to one of the at least two devices where the set of identifiers has a number of identifiers equal to a maximum number of permissible outstanding requests for the one of the at least two devices. A request is received at the storage system from the at least two devices for access to at least one of the plurality of volumes of the storage system. The request includes an encrypted one of the identifiers of the set. Each identifier in the set is used to authenticate a different request from the one of the at least two devices. The request is selectively services at the storage system based at least in part on steps

including verifying that the represented source of the request is the one of the at least two devices that issued the request. The verifying includes determining whether the encrypted one of the identifiers is a next expected identifier of the set. As described below in further detail, it is respectfully submitted that Ericson, Yu, and the APA, taken separately or in any combination, do not disclose or fairly suggest the above-noted features of amended Claim 1.

Ericson discloses a target controller receiving, from an initiator, a probe message including the initiator identifier and the target controller returning a reply message with permitted logical units to the initiator. The initiator also issues an access message including the initiator identifier, target identifier, and the logical units to which access is requested. (See Ericson Figure 2; Col. 4, Line 26-Col. 5, Line 25). However, Ericson is silent regarding the storage system providing a set of identifiers to a device, as recited in the providing step of Claim 1. Ericson is silent regarding any transmission of an access request or access message which includes an encrypted one of the identifiers in the set. Furthermore, Ericson is silent regarding selectively servicing such a request which includes an encrypted one of the identifiers as also recited in the verifying step of Claim 1.

Yu discloses a capability for an object implemented as a data structure where the data structure includes a unique object identifier (UID) and an access right (AR) to the object. (Col. 5, Lines 41-57). Yu discloses use of a signature to protect a transmitted capability to ensure that the transmitted permission cannot be forged. The permission is represented as a capability and a signature. (Figure 3, Col. 6, Line 50-Col. 7, Line 11). Yu teaches that encryption keys may be used in connection with an execution node and a node requesting a capability from the execution node. A different encryption key can be used for each different destination node. (Col. 6, Line 34-Col. 8, Line 60). Yu discloses a procedure for remote access to an object as illustrated in Yu's Figure 4. An object to be accessed is located at an execution node 50. A process requiring access to the object is located at an invocation node 52. The execution node 50 first grants permission to access the object by generating a capability and a signature, and transmitting the capability and

the signature to the invocation node 52. The signature 44 is generated as illustrated in Yu's Figure 5. The granting of permission is associated with contract formation in which selected object accesses are agreed upon. The capability and the signature are stored by the invocation node 52 for future use. At a later time, when the process at the invocation node 52 wishes to access the object at execution node 50, the process transmits the capability, the signature and the identity of the basic service element to the execution node 50. The execution node 50 then authenticates the capability, and if access is authorized, executes the requested basic service element and returns the result to the invocation node 52. (Col. 7, Lines 24-46). The execution node performs the foregoing authentication of a received capability from the transmitting node using the encryption key corresponding to the transmitting node. (Figure 6; Col. 7, Line 46-Col. 8, Line 21). Thus, Yu teaches techniques which, as described above, use a capability, a signature, basic service element identity, and encryption key. However, Yu is silent regarding the storage system providing a set of identifiers to a device, as recited in the providing step of Claim 1. Yu is silent regarding any transmission of an access request or access message which includes an encrypted one of the identifiers in the set where each identifier in the set is used to authenticate a different request from the device. Furthermore, Yu is silent regarding selectively servicing such a request which includes an encrypted one of the identifiers as also recited in the verifying step of Claim 1.

Based on the foregoing, Yu and/or Ericson appear silent regarding any disclosure or suggestion of the above-noted features of Claim 1. Additionally, it is respectfully submitted that the APA is clearly silent regarding any disclosure or suggestion of the above-noted features of amended Claim 1. Thus, Yu, Ericson and the APA, taken separately or in any combination, do not disclose or suggest at least the above-noted features of Claim 1.

For at least the foregoing reasons, Claim 1, and claims that depend therefrom, are neither disclosed nor suggested by the references. Claims 15 and 21, as amended herein, also recite features similar to those above-noted features of Claim 1. Thus, Claims 15

and 21, and claims that depend therefrom, are neither disclosed nor suggested by the references for reasons similar to those set forth above regarding Claim 1.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 15-20 under 35 U.S.C. 103(a) as being unpatentable over Yu is hereby traversed and reconsideration thereof is respectfully requested.

Claim 15, as amended herein, is summarized above. Claims 16-20 depend from Claim 15. For reasons set forth above, Claim 15, and claims that depend therefrom, are neither disclosed nor suggested by Yu, Ericson, and APA, taken separately or in any combination. Thus, it is respectfully submitted that the Yu reference alone does not disclose or suggest amended Claim 15, and claims that depend therefrom, for reasons set forth above.

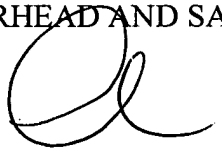
Although Claim 15 is neither disclosed nor suggested by Yu for at least those reasons set forth above, it is noted that Page 14 of the Decision indicates that limitations of Claim 15, prior to amendment herein, directed to how the storage system will use the data structure are considered statements of intended use and not given patentable weight. Accordingly, Claim 15 has been amended herein to recite a computer readable medium comprising stored thereon a first data structure and codes that perform processing as recited in Claim 15. Applicants have amended Claim 15 herein to recite codes stored on the computer readable medium which are entitled to patentable weight by having a functional relationship to the medium. Thus, these recited features are not merely statements of intended use. As such, recited features of Claim 15 previously directed to how the storage system will use the data structure are entitled to patentable weight.

For at least the foregoing reasons, Claim 15, and claims that depend therefrom, are neither disclosed nor suggested by Yu.

In view of the foregoing, Applicant requests that the rejection be reconsidered and withdrawn.

Based on the above, Applicants respectfully request that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 508-898-8604.

Respectfully submitted,
MUIRHEAD AND SATURNELLI, LLC



Date: March 4, 2010

Anne E. Saturnelli
Registration No. 41,290

Muirhead and Saturnelli, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581
Phone: (508) 898-8601
Fax: (508) 898-8602